الحماية من الفيروسات

مقدمة:

شبح الفيروسات مخيف جدا لكل من يعرف مقدار الضرر الذي قد يسببه. الكثيرون لا يدركون مقدار الخطر الذي تشكله الفيروسات الا بعد ان يقوم احد الفيروسات بالتسبب في خسارة كبيرة و خصوصا في الشركات والمصارف.

الوقاية خير من قنطار علاج، و بالتأكيد ان هذا امر لا نقاش فيه عندما يتعلق الامر بالفيروسات، حيث ان ضياع احد الملفات التي تحتوي حسابات الشركة قد يكلفك الكثير من المال لإعادة انشائه، بينما قد تكلفك الوقاية من الفيروسات و الاحتفاظ بنسخة احتياطية من المعلومات المهمة مبلغ من المال لا يكاد يذكر.

كيف تعمل الفيروسات:

لتتمكن من حماية حاسوبك من الفيروسات لا بد لك من معرفة بعض المعلومات عن كيفية عمل الفيروسات و ما هي طبيعتها.

اهم ما يجب معرفته عن الفيروسات هو انها برامج حاسوب، اي انها ليست مخلوقات حية و لا يمكن ان تنتقل من الانسان الى الحاسوب او بالعكس، و من المهم جدا ادراك انه اذا لم يتم تشغيل برنامج الفايروس فانه يبقى ساكنا. تماما كما هو الحال مع كل البرامج الاخرى، مثلا هناك الكثير من الادوات المرفقة مع ويندوز مثل الالعاب لكنها لا تعمل ما لم يتم تشغيلها من قبل المستخدم او من قبل ويندوز او برنامج اخر.

يتم برمجة الفيروسات بحيث تكون قادرة على ربط او الحاق او دمج نفسها مع انواع معينة من الملفات. هذه الملفات هي تلك القابلة للتشغيل. السؤال المهم الان هو ما هي تلك الملفات القابلة للتشغيل:
الملفات القابلة للتشغيل ((هي تلك التي تحتوي على اوامر للمعالج والتي تتطابق صيغتها مع صيغة الملفات القابلة للتشغيل التي يفرضها نظام التشغيل)).
مثلا لا يقوم الفايروس بإدخال نفسه في ملف صورة. حيث ان ملفات الصور لا تحتوي على اوامر للمعالج كما انها لا تحمل الصيغة التشغيلية التي يفرضها ويندوز .
من انواع الملفات التي يمكن ان تحتوي فايروسات: exe, com, doc, dll, drv, fnt, vxd, scr,ocx, vbx, vbs, bat

لنفترض انه وصلك بالبريد الالكتروني ملف قابل للتشغيل يحتوي فايروسا، في حالة انك لم تقم بتشغيل ذلك الملف فان الفايروس لن ينتشر حيث انه لا بد من ان يقوم احد ما بتشغيل الملف الذي يحتوي الفايروس. مثلا اذا قمت بحفظ الملف الذي يحتوي الفايروس او قمت بنسخه او مسحه فان كل هذه العمليات لا تعمل على تشغيل الفايروس. اذا القاعدة الاساسية التي يجب تذكرها دائما هو ان الفايروس لا يبدا بالانتشار اذا لم يتم تشغيله، تذكر ان بعض الملفات يتم تشغيلها تلقائيا من قبل ويندوز كما هو الحال في التشغيل التلقائي او الالي للملفات المستخدمة مع الأقراص المدمجة.

لنفترض انك قمت بتشغيل الملف الذي يحتوي الفايروس دون ان تعلم بوجود الفايروس، في هذه الحالة تكون ايضا قد قمت بتشغيل الفايروس، عندها يعمل الفايروس على تخبئة نفسه في الذاكرة استعدادا لبداء الانتشار. نظرا لان ذاكرة الحاسوب تفقد محتوياتها عند إطفاء الحاسوب فان مبرمج الفايروس يعلم ان على الفايروس ان يقوم بتخزين نفسه على القرص الصلب و كذلك إلحاق نفسه بأحد الملفات التشغيلية ليتم تشغيله تلقائيا عند تشغيل ويندوز، عند تشغيل الفايروس يبقى مختبئا في الذاكرة و يراقب الملفات التي يتعامل معها ويندوز، و عند تشغيل ملف يمكن للفايروس ان يربط برنامجه به يعمل الفايروس على نسخ نفسه بداخل الملف التشغيلي. قد تؤدي عملية نسخ الفايروس لنفسه في داخل الملف التشغيلي الى تخريب ذلك الملف و بالتالي يتوقف عن العمل.
بعض الفيروسات لا تنتظر ان تقوم بتشغيل البرامج و انما تقوم بالبحث عن الملفات المناسبة و تدخل برنامجها في تلك الملفات، و بالتالي فانك عندما تشغل تلك الملفات تكون قد قمت بتشغيل الفايروس.
و عندما تقوم بنسخ احد تلك الملفات لأحد اصدقائك فانك تكون قد نقلت الفايروس الى حاسوبه.

بما ان الفايروس يبقى مختبئا في الذاكرة، فان استعمال برنامجا لمقاومة الفيروسات لن يحل المشكلة حيث ان هذا البرنامج المقاوم للفيروسات سيقع في الأغلب فريسة للفايروس، هل هناك حل لهذه المشكلة؟ اجل هناك حل في الفقرات التالية:-

اذا استخدمت قرصا مدمجا في سواقة الاقراص المدمجة و كان هناك فايروس في برامج الحاسوب فان الفايروس لا ينتقل الى اي من الملفات على القرص المدمج و ذلك لان سواقة الاقراص المدمجة العادية لا تسمح بالكتابة على القرص المدمج.

الوقاية من الفيروسات:

اليك بعض الإجراءات الوقائية التي تساعد في الحماية من الفيروسات:
١- قم بتركيب برنامج للحماية من الفيروسات في ويندوز.
٢- قم دائما بتجديد قاعدة البيانات الخاصة ببرنامج الفيروسات الذي قمت بتركيبه، حيث ان كل يوم يمر قد يبرمج فيه فايروس جديد. الكثير من برامج الوقاية من الفيروسات تمكنك من الحصول على

تجديدات قاعدة البيانات الخاصة بالفيروسات بالمجان من الانترنت، في حالة ظهور فايروس جديد لا يعرف برنامج الوقاية من الفيروسات عنه فانه لا يتمكن من ايجاد ذلك الفايروس.
٣- قبل ان تشغل برنامجا لأول مرة قم بفحصه للتأكد من خلوه من الفيروسات. مثلا يجب ان تقوم بفحص كل الملفات على اي قرص مدمج تشتريه للتأكد من خلو الملفات من الفيروسات، كما يجب ان تسمح لبرنامج الوقاية من الفيروسات بمراقبة كل الملفات اثناء عملية إعداد و تركيب البرنامج و ذلك لإمكانية وجود فايروس مخبئ في احد الملفات المضغوطة.

٤- من الطرق الأكثر شيوعا لنقل الفيروسات و خصوصا عن طريق الانترنت تغيير ايقونة الملف. حيث يقوم الشخص الذي يريد ان ينقل الفايروس الى حاسوبك بتغيير ايقونة الملف التشغيلي الى ايقونة تخص الصور او ملف نصوص مثل ايقونة ملفات مايكروسوفت ورد، و بالتالي فانك تعتقد انه لا يمكن وجود فايروس في هذا الملف و تقوم باستعراض محتوياته لكنك تتفاجئ بان هذا الملف لا يحتوي صورة و ليس ايضا ملف نصوص.

حل هذه المشكلة سهل و بسيط، و هو ان لا تثق بايقونة الملف و انما ان تنظر دائما الى نوعية الملف قبل ان تقوم بتشغيله،اذا يجب عليك ان تطلب من ويندوز ان يعرض دائما نوعية الملفات بالإضافة الى اسمها.
اتبع الخطوات التالية لجعل ويندوز يعرض دائما اسم الملف و نوعه ايضا.
شغل ايقونة My computer ثم اختر من القائمة العلوية Tools ثم اختر من هذه القائمة Folder View. اختر من التبويب العلوي View.
الغي الإشارة من المربع المعنون : Hide file Extensions for Know File Types.
اضغط الزر OK للعودة لحفظ التعديلات. اضغط الزر OK لحفظ التعديلات في هذه الشاشة أيضا.

من الضروري جدا ان تنتبه الى ان نوع الملف هو الذي يكون بعد آخر نقطة من اليسار او قبل أول نقطة من اليمين. اي ان الملف الذي له الاسم صورة نقطة GIF نقطة exe هو ملف قابل للتشغيل و ليس ملف صورة من نوع GIF، تستخدم هذه الطريقة لخداع مستخدمي الانترنت بشكل دائم.

٥- من الطرق السهلة لجدا لنشر فايروس ميزة التشغيل الآلي للبرامج من الأقراص المدمجة. حيث انك بمجرد ان تضع القرص المدمج في السواقة يبدا البرنامج بالعمل دون ان يكون لديك فرصة لفحصه اذا لم يكن لديك برنامج مضاد للفيروسات يراقب الذاكرة باستمرار.
اذا لم تكن تريد ان تتسبب ميزة التشغيل الآلي لك بمشاكل كهذه قم باستخدام برنامج مضاد للفيروسات يتم تشغيله تلقائيا عند تشغيل ويندوز و يبقى في الذاكرة ليراقب كل البرامج و الملفات التي يتم التعامل معها و بالتالي يمكنه ان يكتشف وجود الفيروسات قبل ان يتم تشغيلها، بالطبع لا بد من اتباع النصيحة رقم ٢ اذا كنت تريد حماية حاسوبك من الفيروسات.
يمكنك ان تطفئ ميزة التشغيل الآلي للأقراص المدمجة بإتباع الخطوات التالية:

اضغط بزر الفارة الأيسر فوق إيقونة My Computer ثم اختر من القائمة Properties. اختر من التبويب العلوي في النافذة الجديدة التي تظهر Device Manager. ثم اضغط بزر الفارة الأيسر على إشارة + المجاورة لأيقونة القرص المدمج و الكلمة CDROM. ثم اضغط بزر الفارة الأيسر مرتين متتاليتين على اسم سواقة الأقراص المدمجة الذي ظهر نتيجة الضغط على إشارة +.
اختر من التبويب العلوي Settings ثم الغي الإشارة من المربع المعنون: Auto insert notification.
ثم اضغط الزر OK.
بهذا تكون قد أوقفت ميزة التشغيل التلقائي. اذا اردت ان تستخدم هذه الميزة، اضغط بزر الفارة اليمين على ايقونة سواقة الأقراص المدمجة في My computer ثم اختر من القائمة Auto play.

٦- لا تقم ابدا بتشغيل اي ملف لا تعرف مصدره، حيث انه قد يحتوي على فايروس جديد و بالتالي لن يتمكن برنامج الوقاية من الفيروسات من ايجاد الفايروس.

٧- في حالة ان فايروسا اصاب بعض الملفات و قام برنامج الوقاية من الفيروسات بإلغاء الفايروس من تلك الملفات يفضل ان تقوم بإلغاء تلك الملفات و الحصول على نسخ جديدة منها، حيث ان بعض الفيروسات تخرب الملف الذي تدخل نفسها فيه و بالتالي لا يعود صالحا للتشغيل و قد يصبح هذا الملف في بعض الأحيان خطرا بسبب الضرر الذي لحق به.

٨- اذا توقف ويندوز عن العمل نتيجة وجود احد الفيروسات لا تقم بتركيب ويندوز فوق ويندوز، و إنما بتركيب ويندوز بالطريقة المثالية.

ما هي أعراض الحاسوب المصاب بفيروس أو برنامج ضار؟

ليس من السهل تحديد إذا ما كان الحاسوب مصابا أم لا. حاليا أصبح مبتكرو الفيروسات والبرامج الدودية وأحصنة طروادة وبرامج التجسس يحاولون جاهدين إخفاء أنظمة التشفير وآثار برامجهم على الحاسوب. لذلك من الضروري اتباع هذه الإرشادات وتحديدا قم بتنصيب برامج الحماية وتأكد من أن جميع الرقع الأمنية في نظام التشغيل في حاسوبك تعمل كما قم بنسخ بياناتك إلى أقراص ممغنطة بانتظام.

من الصعب أن تدرج جميع الأعراض الشائعة لإصابة الحاسوب لأن سبب هذه الأعراض قد يكمن في خلل أو عطل في برمجيات أو عتاد الحاسوب. فيما يلي بعض الأمثلة على ذلك:

* حاسوبك يعمل بشكل لم تعهده من قبل.

* تصلك رسائل أو صور غير متوقعة.

* تسمع أصواتا مفاجئة صادرة من حاسوبك.

* بعض البرامج تبدأ بالعمل بشكل تلقائي.

* الجدار الناري الخاص بك ينبئك بأن برنامجا ما حاول الاتصال بالانترنت (وهو ليس البرنامج الذي تشغله).

* بعض من أصدقائك تسلموا رسائل الكترونية أرسلت من بريدك مع أنك لم تقم بإرسالهم أي شيء.

* تزداد حالات "تجمد" الحاسوب، أو يلاحظ بطء في عمل البرامج.

* تصلك رسائل كثيرة بوجود خلل في النظام.

* نظام التشغيل لا يحمّل على حاسوبك لدى تشغيل الجهاز.

* تلاحظ أن ملفاتك أو مجلداتك قد حذفت أو تغيرت.

* يلاحظ وجود اتصال بالقرص الصلب لحاسوبك (يحدد بوجود إحدى الومضات الصغيرة) في الوقت الذي لا تكون تدري بأن برنامجا ما يعمل.

* متصفحك لا يعمل بشكل متواصل، بمعنى أنك لا تستطيع إغلاق نافذة المتصفح.

* تلاحظ انخفاض في المساحة الحرة المتبقية على قرص الصلب :C بالرغم من عدم وجود ما تخزنه من ملفات كبيرة الحجم او كثيرة.

ما الذي يمكننا فعله حيال ذلك؟

لا تقلق إذا وجدت أحد من هذه الأعراض في حاسوبك. قد يكون هناك خلل في القرص الصلب أو البرمجيات الأخرى وليس ناتجا عن فيروس أو ديدان أو حصان طروادة. يجب عليك القيام بالتالي:

اقطع اتصال حاسوبك بالانترنت.

إذا لم يتم تحميل نظام التشغيل الخاص بك، شغل الحاسوب في النظام الآمن (Safe Mode)- عندما تقوم بتشغيل الحاسوب اضغط على المفتاح F8 وواصل الضغط عليه إلى أن تظهر لديك خيارات، اختر من بينها (Safe Mode) أو التشغيل الآمن من خلال قرص الطوارئ.

تأكد من أنك قمت بتحديث مكافح الفيروسات. إذا أمكن لا تنسى أن تقوم بتحميل ما يلزم للتحديث إذا انتابك شك في أن حاسوبك معرض للخطر بشرط أن تستعمل حاسوبا آخر. هذا مهم جدا: إذا كان حاسوبك قد أصيب بفيروس وقمت بالاتصال بالانترنت قد يقوم برنامج ضار بإرسال معلومات هامة إلى مخترق أو ينقلها إلى أجهزة أخرى عن طريق رسائل الكترونية ترسل إلى عناوين صناديق البريد موجودة في جهازك.

إذا كانت لديك أية مشكلة في إزالة البرامج الضارة، راجع الموقع الالكتروني للشركة التي تؤمن لك الحماية في الانترنت للحصول على معلومات حول ما تحتاجه من أدوات لإزالة برنامج ضار ما.

إذا كان حاسوبك الآلي متصل بشبكة محلية قم بقطع الاتصال.

قم بفحص الحاسوب كاملا.

إذا وجدت برنامجا خبيثا اتبع التعليمات الموجودة لدى مكافح البرامج الخبيثة الذي تستعمله. برامج الحماية الجيدة تقوم بـ"تطهير" الأجزاء المصابة، وعزل الأجزاء التي يشك بأنها مصابة وحذف البرامج الدودية وأحصنة طروادة. كما أنها تقدم تقريرا بأسماء الملفات المصابة والبرامج الضارة التي قد تكتشف في الحاسوب.

إذا كانت برنامج الحماية من مخاطر الانترنت لم تكتشف أي خطر فهذا يعني أن جهازك غير مصاب. تأكد من أن برمجيات وعتاد الحاسوب (قم بإزالة البرمجيات غير المرخصة والملفات البالية) وتأكد من أنك تعمل بنظام تشغيل حديث وقمت بتنصيب الرقع الأمنية.

إن استدعت الضرورة اتصل بدائرة الدعم الفني للشركة التي توفر لك الحماية من مخاطر الانترنت للحصول على تعليمات إضافية. بإمكانك أن تسأل عن كيفية اختبار ملف ما لتحليله من قبل باحث الفيروسات.

اعداد

عادل الزبيدي